

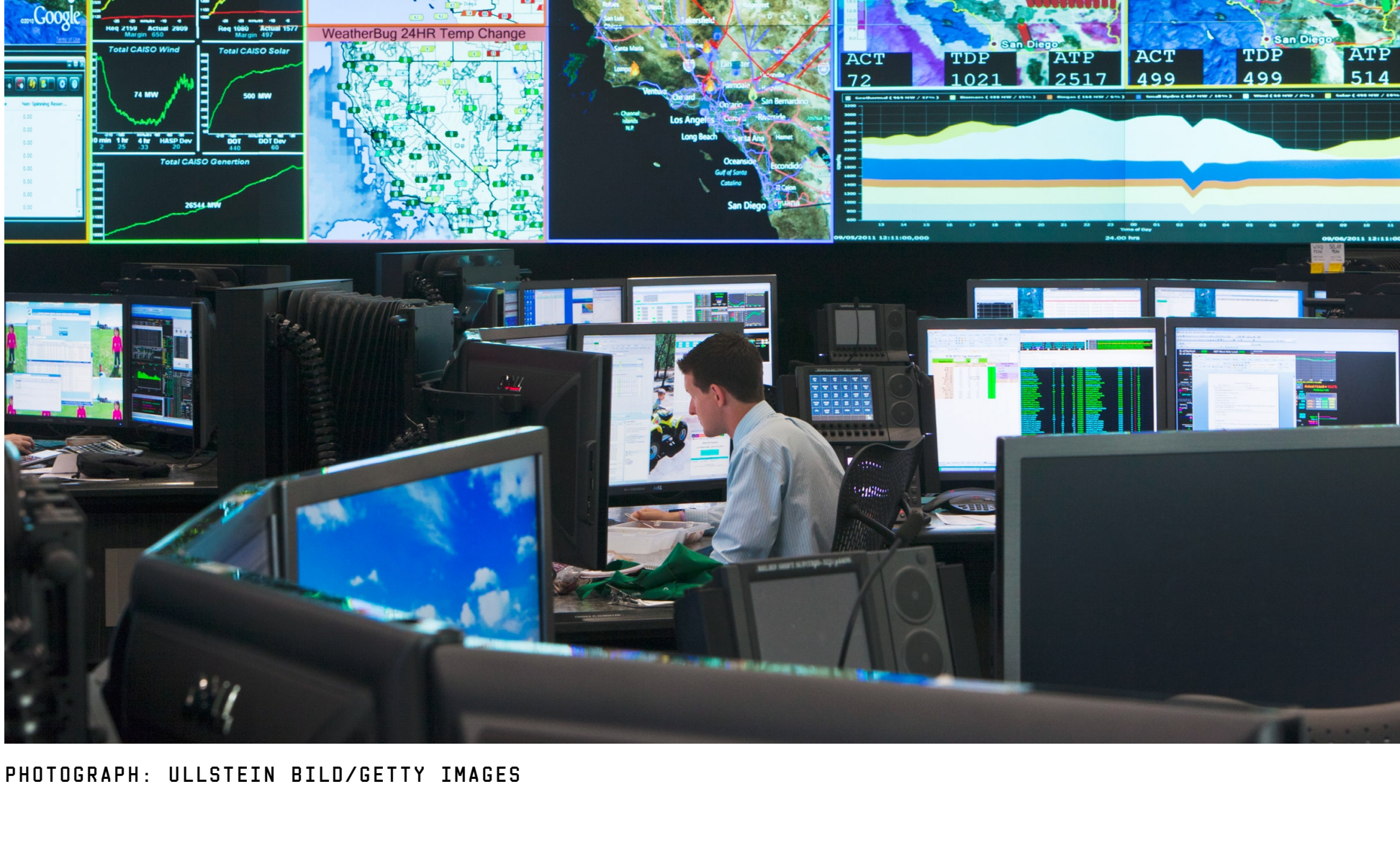
BRIAN BARRETT

SECURITY

09.07.2019 10:00 AM

# Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities

Exposed Facebook phone numbers, an XKCD breach, and more of the week's top security news.



PHOTOGRAPH: ULLSTEIN BILD/GETTY IMAGES

**THIS WEEK SAW** some aftershocks from recent revelations about a [large-scale iOS hacking campaign](#). Brokers of so-called zero day exploits—the kind that companies haven't yet patched—have started [charging more for Android hacks](#) than iOS for the first time. And [Apple finally released a statement](#) that both criticized Google's characterization of the attacks and downplayed the significance of the targeted surveillance of at least thousands of iPhone owners.

We took a look at a [bug in Supermicro hardware](#) that could let hackers pull off a USB attack virtually. Google [open-sourced its differential privacy tool](#), to help any company that crunches big data sets invade your privacy less in the process. And speaking of privacy, we detailed the [11 settings you need to check on Windows 10](#) to preserve yours.

And while it feels like forever ago that Jack Dorsey's Twitter account got hacked, it's [worth revisiting exactly how it happened](#). (Twitter this week closed the texting loophole at the heart of it.) We also took a look at [Jeremy Renner's content moderation woes](#). Bet you weren't expecting to see that sentence in your lifetime.

And there's more! Every Saturday we round up the security and privacy stories that we didn't break or report on in-depth but which we think you should know about nonetheless. Click on the headlines to read them, and stay safe out there.

## Hackers Hit US Power Utilities With a Cyberattack

Let's not overplay this: There was no blackout, and it's not even clear that it was a specifically targeted attack. But hackers *did* use firewall vulnerabilities to cause periodic "blind spots" for grid operators in the western US for about 10 hours on March 5. It's the first known time a cyberattack has caused that kind of disruption—which, again, did not affect the actual flow of electricity—at a US power grid company. The incident was originally referenced in a Department of Energy [report](#) in April, but only in vague terms. A new North American Electric Reliability Corporation document described it in more detail, including the type of vulnerabilities that let hackers compromise the web portals in question. No need to panic about this incident specifically, but given the extent to which [Russia and others](#) continue to probe the power grid, it's an unsettling reminder that weaknesses are out there.

## Database With Over 400 Million Facebook User Phone Numbers Sat Exposed Online

A security researcher found a database containing 419 million or so phone numbers associated with Facebook accounts, yet another in a long string of Facebook losing control of the sensitive data with which you entrust it. Facebook told TechCrunch that the data set is "old," which isn't especially useful, for the obvious reason that most people don't change their phone numbers very often.

## DMVs Are Selling Driver Data to Private Buyers

Through public records requests, Motherboard has determined that when you give your name and address to the DMV, some of those agencies will sell it to private investigators. Several DMVs told Motherboard that at least they don't also sell user photos and Social Security numbers, which, thanks? But they do sell records for as little as a penny. And all of this is somehow legal! Something else to fume about the next time you're in line for a registration renewal.

## Feds Demand App Stores Cough Up Names of Gun Scope App Users

According to court documents uncovered at Forbes, federal investigators have requested that Apple and Google turn over information about people who downloaded a gun scope app Obsidian 4. That's at least 10,000 on the Google Play Store alone. It's part of a broader look into potential breaches of weapons export regulations, but privacy advocates have raised understandable concerns over the many thousands of totally innocent people who would be caught up in such a sweeping request.

## Killjoy Hackers Compromised the XKCD Forums

Beloved [internet comic XKCD](#) had its fan forums breached recently; 560,000 usernames, email addresses, and IP addresses were taken. That makes it a relatively small hack in the grand scheme of things, but still disappointing that someone chose that as a target. XKCD is great, leave it alone!

## More Great WIRED Stories

- Nobody's watching the best [giant monster movies](#)
- How to get the most [out of your smartphone battery](#)
- You're [racing toward a wall](#). Should you brake hard—or swerve?
- A history of plans to [nuke hurricanes](#) (and other stuff too)
- For these [sword-wielding warriors](#), medieval battles live on
- 🕵️ Facial recognition [is suddenly everywhere](#). Should you worry? Plus, read the [latest news on artificial intelligence](#)
- ✨ Optimize your home life with our Gear team's best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#).

**Brian Barrett** is the digital director at WIRED, covering security, consumer technology, and anything else that seems interesting. Prior to WIRED he was the editor in chief of the tech and culture site Gizmodo and was a business reporter for the Yomiuri Shimbun, Japan's largest daily newspaper.

DIGITAL DIRECTOR

t

## Featured Video

WATCH

Hacker Breaks Down 26 Hacking Scenes From Movies & TV

**Hacker Breaks Down 26 Hacking Scenes From Movies & TV**  
Hacker and security researcher Samy Kamkar takes a look at a variety of hacking scenes from popular media and examines their authenticity.

TOPICS

SECURITY ROUNDUP

POWER GRID

HACKING

# News of the future, now.

Get WIRED

SUBSCRIBE

WIRED

WIRED is where tomorrow is realized. It is the essential source of information and ideas that make sense of a world in constant transformation. The WIRED conversation illuminates how technology is changing every aspect of our lives—from culture to business, science to design. The breakthroughs and innovations that we uncover lead to new ways of thinking, new connections, and new industries.

## MORE FROM WIRED

Subscribe  
Newsletters  
FAQ  
Wired Staff  
Press Center

## CONTACT

Advertise  
Contact Us  
Customer Care  
Send a tip securely to WIRED  
Jobs

